VPN Basics

Table of Contents

Introduction

The VA offers remote desktop access to VA network resources through a Virtual Private Network (VPN) utilizing the Citrix Access Gateway (CAG). CAG can be used from any accessible computer with an internet connection.

By having a VPN account, you can access the Omaha Desktop to run common applications found already on all VA computers (i.e. VistA, CPRS, MS Office Suite). You will also be able to access shared drives like your P: drive, S: drive, and the Research Server. Additionally, the MS Outlook e-mail client can be used to access your VA e-mail, and intranet sites, including SharePoint, can be accessed.

When you VPN in to the VA network, you can do nearly all computer-related tasks through CAG that you might do at an actual VA desktop computer with three exceptions; *File transferring* (from one desktop to another), *printing to local or LAN printers*, and a *limited desktop profile* (storage space for files and shortcuts placed on the remote desktop).

VPN and VA network accounts are managed separately. It is recommended that you log in to CAG periodically. After 90 days of inactivity, the VPN account will be disabled.

Requesting a VPN Account

Please follow these steps to request and establish a VPN account from the Information Security Officer (ISO)

1. Send an e-mail to the Research ADPAC requesting a VPN account. Your User Access Form (UAF) will need to be updated.

2. Using a VA computer, go to the following website: https://vpnportal.vansoc.va.gov/SelfService/. It is behind the VA firewall and cannot be accessed from outside the VA network.

3. Log in using your VA Windows credentials and provide the requested information. Use the VA Research ACOS as your supervisor.

4. The approval process usually takes less than five work days. If approved, you will receive an e-mail from the ISO through your VA e-mail account with further instructions.

   NOTE: Once approved, you have until

Accessing the Citrix Access Gateway (CAG)

Although detailed instructions will be provided from the ISO for VPN access, the following steps may be a little bit more straight forward. Assuming you have a confirmed VPN account, perform the following:

1. Open your internet browser. Supported browsers:
   - Internet Explorer (between 6.0 and 8.0.)
   - Mozilla Firefox (3.6.x.x and above.)
   - Safari on Mac (5.0 and above.)

2. Open the browser's internet option dialog
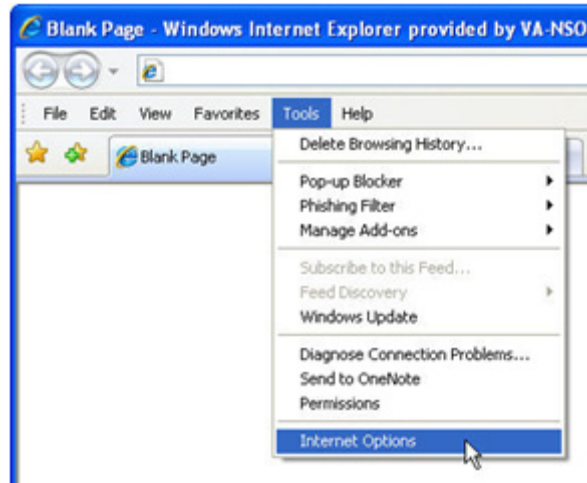
3. From the Internet Options window, select the Advanced tab. Scroll down to the "Use TLS 1.0" selection and be sure it is checked as shown.
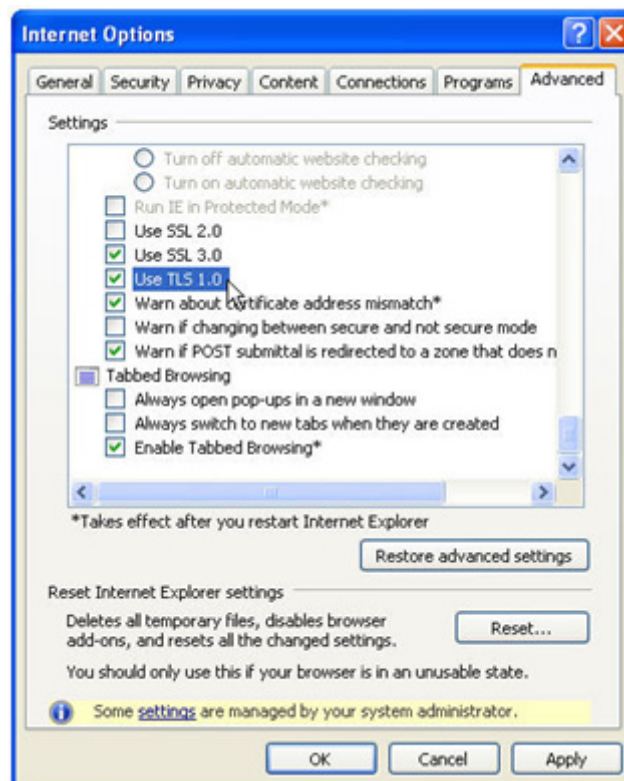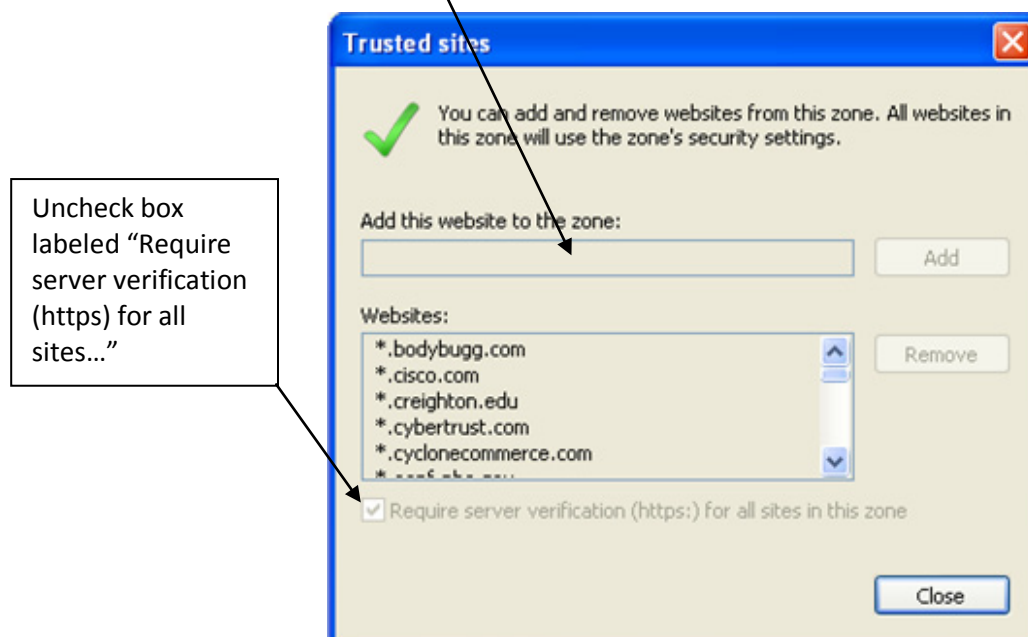
4. 1) Select the Security tab. 2) Select Trusted Sites and then 3) click on the Sites button
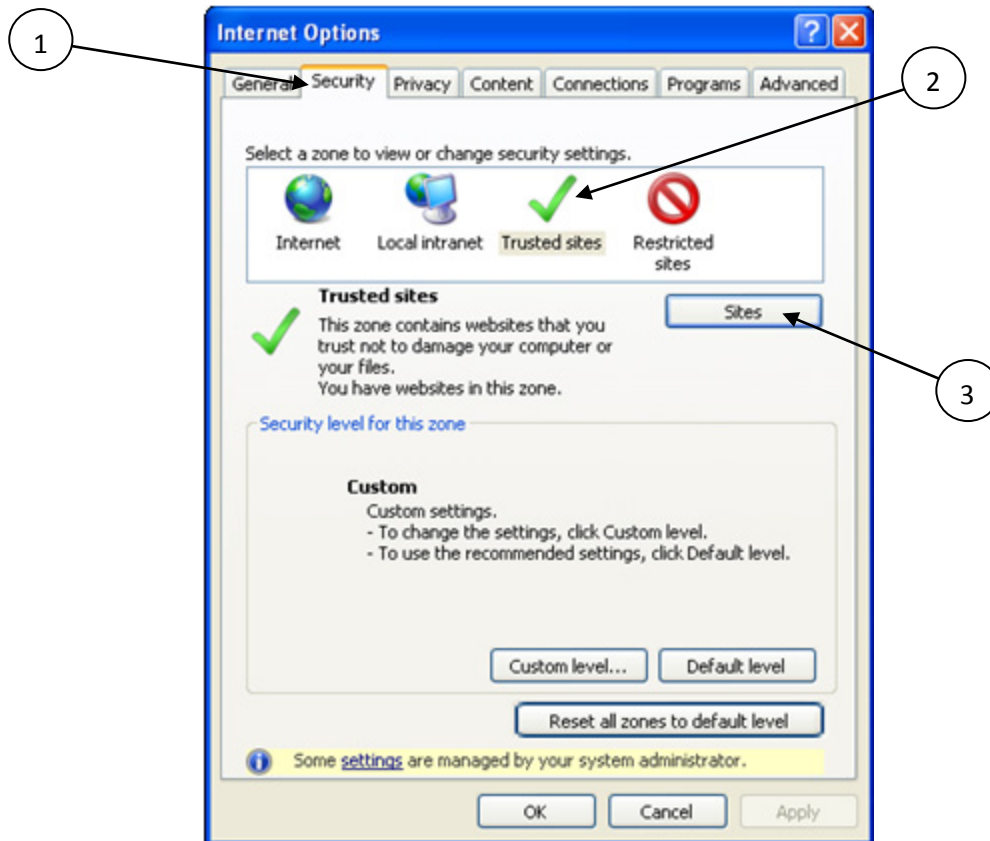

5. One at a time, add the following websites to the Trusted Sites Zone:

https://var.vpn.va.gov
http://var.vpn.va.gov
https://vareast.vpn.va.gov
https://varnorth.vpn.va.gov

Uncheck box labeled "Require server verification (https) for all sites..."

6. Click "Close" and click "OK" to close the internet options dialog.

7. Enter https://vareast.vpn.va.gov OR https://varwest.vpn.va.gov into the browser's address bar. Enter https://varnorth.vpn.va.gov if you are using a MAC. Press Enter.
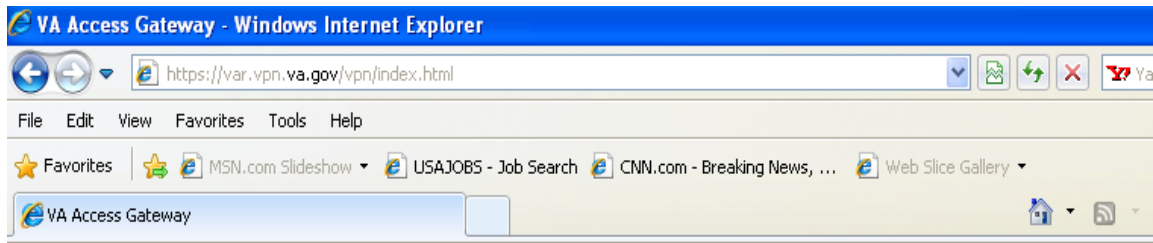
8. You'll be presented with the CAG Screen

Enter your VA Windows login credentials in the form of Domain\Username (i.e. vha23\vhaomauser).

9. If logging in for the first time on the computer you are using, you will be prompted to install Citrix XenApp.
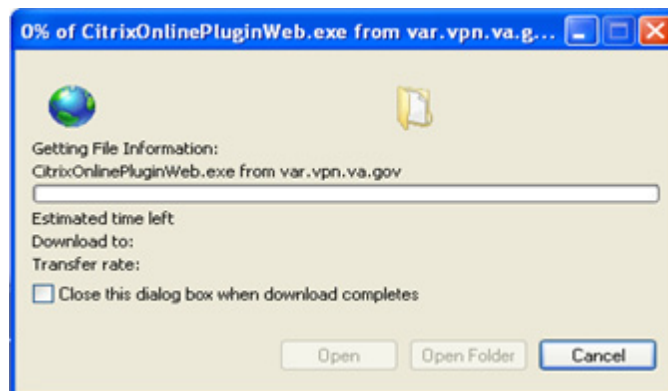

Be sure to check the box "I agree with the Citrix license agreement.

10. The Plug-in for your web browser will download and install.

Internet Explorer v6.0 – 8.0 and Firefox v1.x – 5.x are the currently supported browsers with this plug-in.

Supported operating systems include Windows 7, XP, Vista, Mac OS X v10.4-10.6 (32 & 64-bit)

11. Once the plug-in has been installed, the VISN resource page will be displayed.
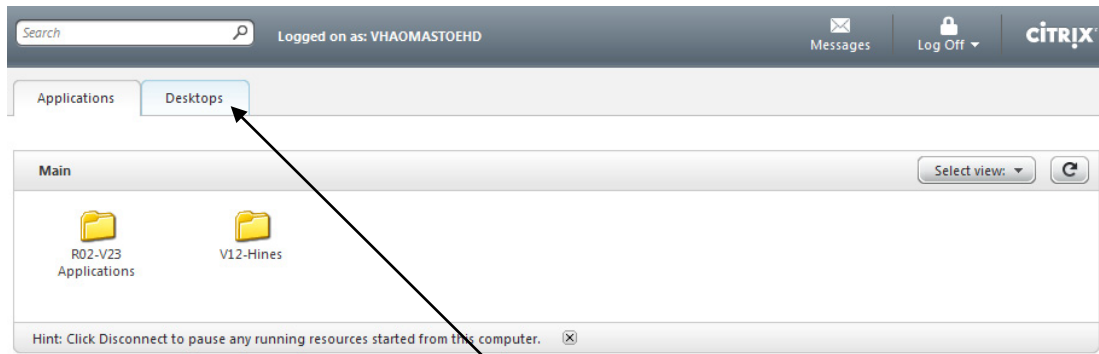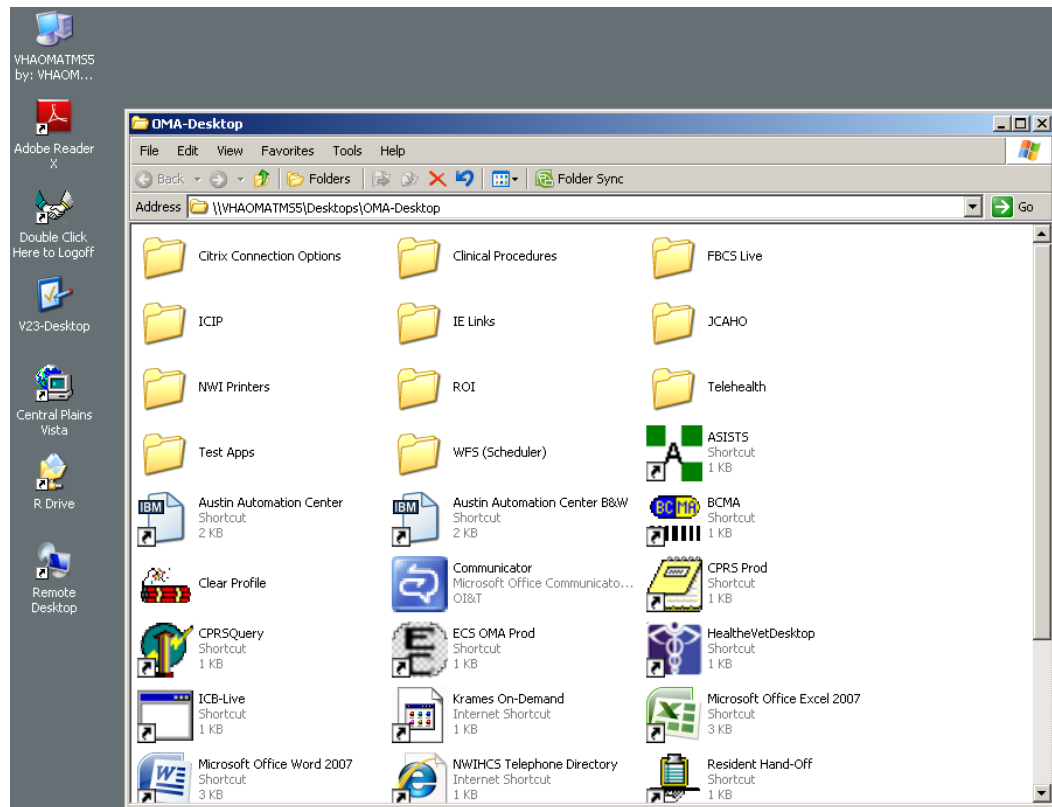

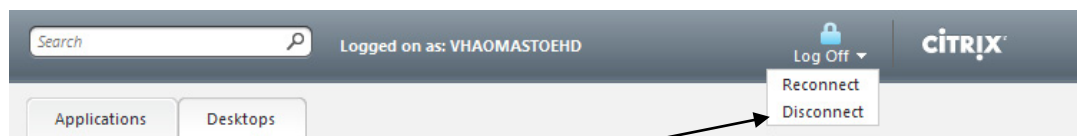Click on the <u>Desktops</u> tab

12. Click the OMA-DESKTOP

13. After Citrix establishes a connection with the VISN 23 desktop, you will see something like this:

14. To log off, close the remote desktop itself,

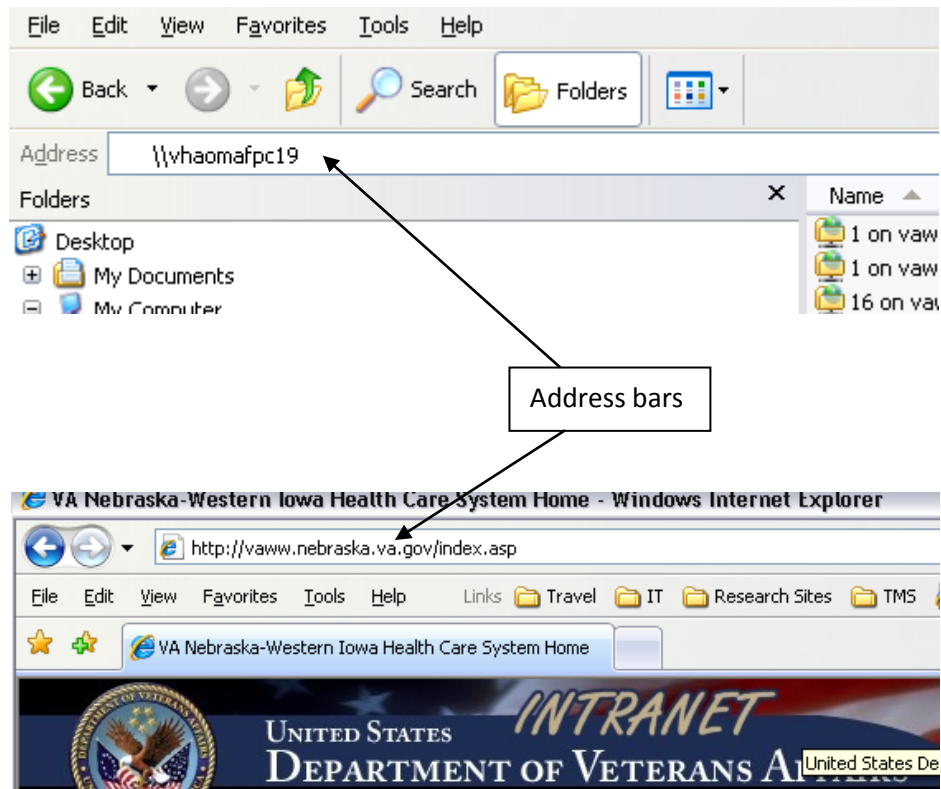Or, click on this icon on the desktop:

Next: Disconnect from CAG

Tips and Tricks

Shortcuts vs. Direct Address Entries

1. Entering the location of a file or application on a server in the address bar of file explorer or Internet Explorer will not work (you end up with a permissions error).


Instead…Create a shortcut to the location on your desktop of folder. HINT: You might want to refer to the shortcuts you have already made in either your Favorites or Desktop folders by making a copy of them and placing them on your P: drive (this is explained below).

Back up Your "Favorites" and "Desktop" Folders to Your P: Drive

Making a backup of your "Favorites" and "Desktop" folders to your P: drive should be a task performed on a routine basis. In the case where your VA computer needs to be replaced or re-imaged (everything you have on the computer is wiped clean and started over), you can save a great deal of time by simply copying your backups back on to the new machine. Having a copy of these folders on your P: drive also makes them accessible when you VPN into the VA network.

Here's how:

1. Go to the file Explorer and find your username in the following location: C:\Documents and Settings
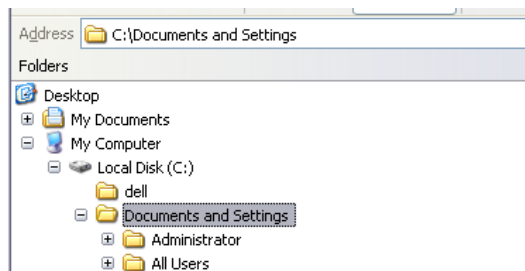
2. Open your folder and highlight the "Desktop" folder and "Favorites" folder (use Ctrl-left-click to select more than one folder at a time).
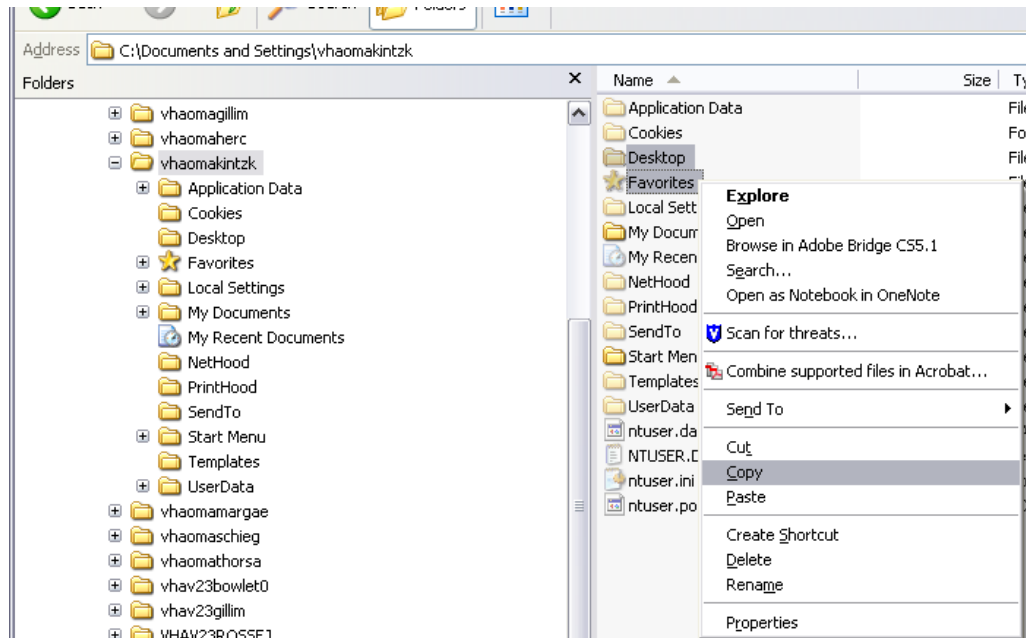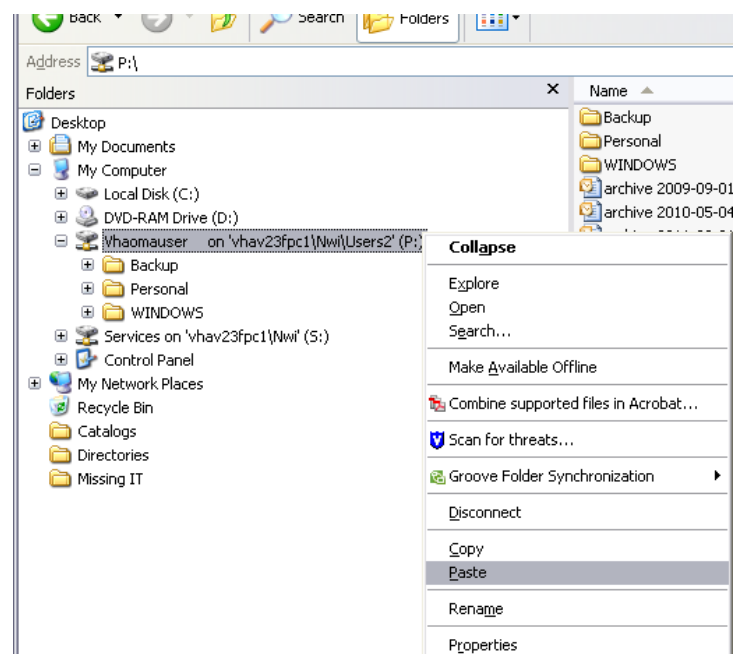

3. Right-click on the highlighted folders and copy
4. Go to your P: drive. Right-click on the highlighted P: drive and paste.

Troubleshooting

Problem	Possible Solution
Citrix software will not download from internet.	Connect to: https://rescue.vpn.va.gov/ViewDocuments/CAGMedia.aspx Download the client that you need, save to PC, then run.
The location of a server is typed into the address bar but error message indicates no permissions.	This is a known bug. As a work-around, create shortcuts with the location information. Follow the steps under "Tips and Tricks - Shortcuts vs. Direct Address Entries"
Can't log in. Account disabled.	1) Contact the Information Security Officer (ISO), Stephen Quinn. Ph: (402) 995-3858, Stephen.Quinn2@va.gov

2) Call the VPN Help Desk directly at (800) 877-4328.

NOTE: It is recommended that you log in to VPN prior on the same day that your account is re-enabled to avoid the account from being reset again. To avoid this problem of disabled accounts, users are reminded to VPN in on a regular basis. After 90 days of inactivity, the account will be disabled. |
| Can't open e-mail. Outlook does not appear to recognize my name. | Mail options may need to be manually configured. Open the "Mail" icon in the Control Panel and make sure that the Microsoft Exchange server is VHAV23MSGA3.v23.med.va.gov Enter your username and click the "Check Name" button. Also, open the "More Settings…" dialog and enter your VA e-mail address.

As a work-around, the VA has a Web-mail site: https://webmail.va.gov/ exchweb/bin/auth/owalogon.asp? url=https://webmail.va.gov/exchange/&reason=0 |
| I can't see my "Personal Folders" in Outlook. | Within Outlook, go to Tools → Account Settings → Data Files tab. Add "Personal Folders.pst" located on your P: drive. |
| Have not received any feedback from ISO on status of VPN account request. | 1) Review any information that may be available at the following site: https://vpnportal.vansoc.va.gov/SelfService/

2) Contact the Information Security Officer (ISO), Stephen Quinn. Ph: (402) 995-3858, Stephen.Quinn2@va.gov |

VA Remote Access Policy

It is the responsibility of the user who has been granted remote access to VA resources to read and understand the following:

VA Remote Access Policy

VA Handbook 6500 places restrictions on VA remote access users. Please review the following :
Handbook 6500 Information Security Program (PDF)
      6500 Appendix A, Terms and Definitions (PDF)
      6500 Appendix B, Acronyms (PDF)
      6500 Appendix C, References (PDF)
      6500 Appendix D, Minimum Security Controls For VA Information Systems (PDF)
      6500 Appendix E, VA Control Configuration Standards (PDF)
      6500 Appendix F, VA Password Management (PDF)
      6500 Appendix G, VA National Rules Of Behavior (PDF)

Users are encouraged to read the entire VA 6500 Handbook and other remote access compliance documentation located at https://rescue.vpn.va.gov. If your remote access environment does not comply with the requirements outlined in the Handbook or your remote access needs are not addressed in an approved waiver, then you are not an authorized remote access user. If you have questions pertaining to this policy or your remote access status, please contact your Information Security Officer (ISO), Stephen Quinn.

Remote Access Software and Documentation

Remote access software, supporting documentation, FAQs and general information are hosted at the VA's Remote Access web site found at https://rescue.vpn.va.gov. Please ensure you have TLS 1.0 enabled on your web browser before attempting to access this site. To enable TLS within Internet Explorer: Select 'Tools', then 'Internet Options', then the 'Advanced' tab. Enable the checkbox for 'Use TLS 1.0' (found towards the end of the list). This web site is password protected - you will need to provide your VA windows login credentials and password before you can gain access.